UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/754,190	01/05/2001	Chiaki Tanimoto	XA-9418	3616

181 7590 05/24/2004

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
SONG, HOSUK	
ART UNIT	**PAPER NUMBER**
2135	6

DATE MAILED: 05/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/754,190	TANIMOTO ET AL.
	Examiner	Art Unit
	Hosuk Song	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-13 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-13 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 1/5/01 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 2.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

1. Regarding claims 2,4,6,8, the phrase "or the like" renders the claim(s) indefinite because the claim(s) include(s) elements not actually disclosed (those encompassed by "or the like"), thereby rendering the scope of the claim(s) unascertainable. See MPEP § 2173.05(d).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1,3,9,11 are rejected under 35 U.S.C. 102(b) as being anticipated by Ohuchi(US 4,864,491).

Claim 1: Ohuchi discloses IC card supplied with an operating voltage by an electrical connection between each of external terminals and a read/write device in (fig.3 and col.3,lines7-22) and including an input-output operation of data with an encoding process or a decoding process executed by an encoding processing computing unit operated in response to instructions issued from a central processing unit in (col.5,lines 26-56). Ohuchi discloses encoding process processing unit is provided with each of registers, which stores data used for a computation for the encoding process or decoding process in plural bit units, and data necessary prior to the encoding process or the decoding process is stored in the register in (col.3,lines 35-52).

Claim 3: Ohuchi discloses an IC card supplied with an operating voltage by an electrical connection between each of external terminals and a read/write device in (fig.3 and col.3,lines7-22) and including an input-output operation of data with an encoding process or a decoding process executed by an encoding processing computing unit operated in response to instructions issued from a central processing unit in (col.5,lines 26-56). Ohuchi discloses encoding processing unit has a signal path for capturing data used for the next computation from a storage circuit concurrently with a computing operation for the encoding process or decoding process in (col.1,lines 19-23;col.3,lines 7-52).

Claim 9: Ohuchi discloses a microcomputer having a module configuration including an input-output operation of data with an encoding process or a decoding process executed by an encoding processing computing unit operated in response to instructions given from a central processing unit in (col.3,lines 23-52). Ohuchi discloses encoding process processing unit is provided with each of registers, which stores data used for a computation for the encoding process or decoding process in plural bit units, and data necessary prior to the encoding process or the decoding process is stored in the register in (col.3,lines 35-52).

Claim 11: Ohuchi discloses a microcomputer having a module configuration including an input-output operation of data with an encoding process or a decoding process executed by an encoding processing computing unit operated in response to instructions given from a central processing unit in (col.3,lines 23-52). Ohuchi disclose encoding processing computing unit has a signal path for capturing data used for the next computation from a storage circuit concurrently with a computing operation for the encoding process or decoding process in (col.1,lines 19-23;col.3,lines 7-52).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 2,4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ohuchi(US 4,864,491) in view of Curiger et al.(US 6,064,740).

Claim 2: Ohuchi does not specifically discloses exponential residue multiplying operation applicable to RSA cryptography and computing A=A^2 Mod N and A=ABModN with A=1 and B=X in response to plural bits as viewed by a plural bits from a high order of Y upon computation and brings the value of B necessary for the computation of ABmodN from the register in association with combinations of the plural bits. Curiger's patent discloses modulo exponentiation calculations in an integrated circuit applicable to RSA cryptography and discloses encoding process above in (col.9,lines 31-41;col.10,lines 15-56). It would have been obvious to person of ordinary skill in the art at the time invention employ exponential residue multiplying operation applicable to RSA cryptography as taught in Curiger with IC card disclosed in Ohuchi in order to perform high speed modulo exponentiation and accommodate exponentiation of very large operands while limiting the required gate density per IC device which offers advantages for public key encryption systems for real time applications.

Claim 4: Ohuchi does not specifically discloses exponential residue multiplying operation applicable to RSA cryptography and computing A=A^2 Mod N and A=ABModN with A=1 and B=X in response to plural bits as viewed by a plural bits from a high order of Y upon computation and brings the value of B necessary for the computation of ABmodN from the register in association with combinations of the plural bits. Curiger's patent discloses modulo exponentiation calculations in an integrated circuit applicable to RSA cryptography and discloses encoding process above in (col.9,lines 31-41;col.10,lines 15-56). It would have been obvious to person of ordinary skill in the art at the time invention employ exponential residue multiplying operation applicable to RSA cryptography as taught in Curiger with IC card disclosed in Ohuchi in order to perform high speed modulo exponentiation and accommodate exponentiation of very large operands while limiting the required gate density per IC device which offers advantages for public key encryption systems for real time applications.

4. Claim 5,7,12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ohuchi(US 4,864,491) in view of Bitoh(US 4,804,825).

Claim 5: Ohuchi discloses an IC card which is supplied with an operating voltage by an electrical connection between each of external terminals and a read/write device in (fig.3 and col.3,lines7-22) and input-output operation of data with an encoding process or a decoding process executed by an encoding processing computing unit operated in response to instructions issued from a central processing unit in (col.5,lines 26-56). Ohuchi discloses central processing unit supplies a leading address at which data for the encoding or decoding process is stored, to the storage circuit, and storage circuit reads data, based in an address signal formed by a built-in address generating circuit based on the leading address and transfers the same to the encoding processing unit in (fig.3 and col.7-59). Ohuchi does not specifically disclose random number generator commonly connected with the central processing unit. Bitoh's patent discloses random number generator in IC card connected with CPU in (fig.2 and col.6,lines 40-43). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ a random number generator as taught in Bitoh with IC card disclosed in Ohuchi in order to generate a non-deterministic numbers which is immune to attack and compromise and challenge is maintained secure and available for further secure communication between devices.

Claim 7: Ohuchi discloses an IC card which is supplied with an operating voltage by an electrical connection between each of external terminals and a read/write device in (fig.3 and col.3,lines7-22) and input-output operation of data with an encoding process or a decoding process executed by an encoding processing computing unit operated in response to instructions issued from a central processing unit in (col.5,lines 26-56). Ohuchi discloses central processing unit supplies a leading address at which data for the encoding or decoding process is stored, to the storage circuit, and storage circuit reads data, based in an address signal formed by a built-in address generating circuit based on the leading address and transfers the same to the encoding processing unit in (fig.3 and col.7-59). Ohuchi does not specifically disclose random number generator commonly connected with the central processing unit. Bitoh's patent discloses random number generator in IC card connected with CPU in (fig.2 and col.6,lines 40-43). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ a random number generator as taught in Bitoh with IC card disclosed in Ohuchi in order to generate a non-deterministic numbers which is immune to attack and compromise and challenge is maintained secure and available for further secure communication between devices.

Claims 12,13: Ohuchi discloses a microcomputer and input-output operation of data with an encoding process or a decoding process executed by an encoding processing computing unit operated in response to instructions issued from a central processing unit in (col.5,lines 26-56). Ohuchi discloses central processing unit supplies a leading address at which data for the encoding or decoding process is stored, to the storage circuit, and storage circuit reads data, based in an address signal formed by a built-in address generating circuit based on the leading address and transfers the same to the encoding processing unit in (fig.3 and col.7-59). Ohuchi does not specifically disclose random number generator commonly connected with the central processing unit. Bitoh's patent discloses random number generator in IC card connected with CPU in (fig.2 and col.6,lines 40-43). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ a random number generator as taught in Bitoh with IC card disclosed in Ohuchi in order to generate a non-deterministic numbers which is immune to attack and compromise and challenge is maintained secure and available for further secure communication between devices.

5. Claims 6,8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ohuchi(US 4,864,491) in view of Bitoh(US 4,804,825) and further in view of Curiger et al.(US 6,064,740).

Claim 6: Neither Ohuchi nor Bitoh specifically discloses exponential residue multiplying operation and computing A=A^2 Mod N and A=ABModN with A=1 and B=X in response to plural bits as viewed by a plural bits from a high order of Y upon computation and brings the value of B necessary for the computation of ABmodN from the register in association with combinations of the plural bits. Curiger's patent discloses modulo exponentiation calculations in an integrated circuit applicable to RSA cryptography and discloses encoding process above in (col.9,lines 31-41;col.10,lines 15-56). It would have been obvious to person of ordinary skill in the art at the time invention employ exponential residue multiplying operation applicable to RSA cryptography as taught in Curiger with IC card disclosed in Ohuchi and Bitoh in order to perform high speed modulo exponentiation and accommodate exponentiation of very large operands while limiting the required gate density per IC device which offers advantages for public key encryption systems for real time applications.

Claim 8: Neither Ohuchi nor Bitoh specifically discloses exponential residue multiplying operation and computing A=A^2 Mod N and A=ABModN with A=1 and B=X in response to plural bits as viewed by a plural bits from a high order of Y upon computation and brings the value of B necessary for the computation of ABmodN from the register in association with combinations of the plural bits. Curiger's patent discloses modulo exponentiation calculations in an integrated circuit applicable to RSA cryptography and discloses encoding process above in (col.9,lines 31-41;col.10,lines 15-56). It would have been obvious to person of ordinary skill in the art at the time invention employ exponential residue multiplying operation applicable to RSA cryptography as taught in Curiger with IC card disclosed in Ohuchi and Bitoh in order to perform high speed modulo exponentiation and accommodate exponentiation of very large operands while limiting the required gate density per IC device which offers advantages for public key encryption systems for real time applications.

6. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ohuchi(US 4,864,491).

Claim 10: Ohuchi does not specifically disclose module configuration is formed on one semiconductor substrate for the implementation. Official notice is taken that module configuration is formed on one semiconductor substrate for the implementation is well known in the art. One of ordinary skill in the art would have been motivated to use semiconductor substrate because it offers high speed and low power consumption.

Information Disclosure Statement

7. The information disclosure statement filed 1/5/01 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each U.S. and foreign patent; each publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed.(The Smart Card Handbook, pp 262-63 missing). It has been placed in the application file, but the information referred to therein has not been considered.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hosuk Song whose telephone number is 703-305-0042. The examiner can normally be reached on Tue-Fri from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HS

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100